Research Paper Engineering

# Implementation of Eigrp Protocol in Wireless Sensor Networks for Energy-Efficient Clustering

**S. Balaji** | Assistant Professor, CSE

**C.Dipthi** | Assistant Professor, CSE

**ABSTRACT**

The Wireless Sensor Networks popularity has increased tremendously, which will connect the virtual world with physical world by its vast potential of the sensor nodes. If the sensor nodes placed in hostile environments once then replacing them is become a tedious task since they rely on battery power. Once those device starts sensing the environment it will sense all the data including noise present within the environment which leads impact on data loss since sensor node provide limited data storage. Also hackers can easily hack the data while transmitting to sink since sensor nodes has no secure transmission aspects. Thus, improving energy of these networks, data storage and secure transmission becomes important in WSN. So methods for clustering and cluster head selection to improve its energy efficiency, SNR values determination to avoid noisy data storage and hash key function attached with data for secure data transmission should be provided in WSN. Enhanced Interior Gateway Routing Protocol (EIGRP), protocol architecture for heterogeneous WSNs was developed which combines the ideas of energy-efficient cluster-based routing with data aggregation, SNR functionalities and MD5 hash methodologies together to achieve good performance in terms of system lifetime, latency, and application-perceived quality.

**KEYWORDS** | WSN, EIGRP, SNR, MD5, clustering, energy efficiency

## 1. INTRODUCTION

A Wireless Sensor Network or WSN is supposed to be made up of a large number of sensors and at least one base station. The sensors are autonomous small devices with several constraints like the battery power, computation capacity, communication range and memory. They also are supplied with transceivers to gather information from its environment and pass it on up to a certain base station, where the measured parameters can be stored and available for the end user.

In most cases [1,2], the sensors forming these networks are deployed randomly and left unattended to and are expected to perform their mission properly and efficiently. As a result of this random deployment, the WSN has usually varying degrees of node density along its area. Sensor networks are also energy constrained since the individual sensors, which the network is formed with, are extremely energy-constrained as well. The communication devices on these sensors are small and have limited power and range.

Both the probably difference of node density among some regions of the network and the energy constraint of the sensor nodes cause nodes slowly die making the network less dense. Also it is quite common to deploy WSNs in harsh environment, what makes many sensors inoperable or faulty. For that reason, these networks need to be fault-tolerant so that the need for maintenance is minimized.

Typically the network topology is continuously and dynamically changing, and it is actually not a desired solution to replenish it by infusing new sensors instead the depleted ones [3]. A real and appropriate solution for this problem is to implement routing protocols that perform efficiently and utilizing the less amount of energy as possible for the communication among nodes.

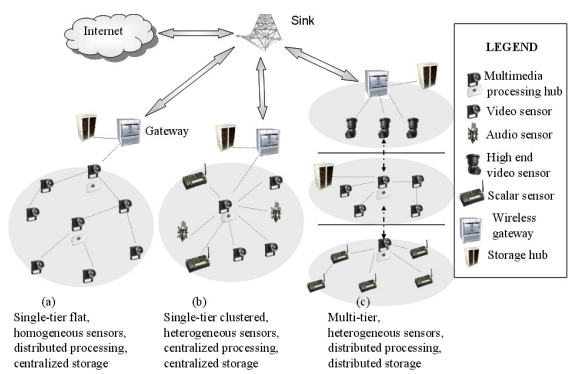


**FIGURE 1.1: Wireless Sensor Network**

The WSN consist of two main components:
1. Sensor Nodes, and
2. Base Station (Central Gateway).

The applications for WSNs are several and various [4]. They are used in scalable also monitor data that manufacturing applications to would be complex costly to screen using wired sensors. They may possibly be deployed in desert area the monitor several environmental unpredictable without the need to refresh and change their power supply would remain for many years. They may possibly form a boundary regarding a possession monitor the development of intruder in the temporary in sequence from one node to another node. Hereby lot of uses for WSNs. These type applications of WSNs consist of tracking, controlling, monitoring. The numbers of functions are environment monitor, traffic monitoring, object tracking, nuclear reactor calculating traffic monitoring fire detection etc. In a typical application a WSNs is extend in area +where it is intended to gathering information throughout its sensor nodes.

Green monitor
Haunt monitor
Services surveillance
Record tracking
Health check monitoring
Smart spaces

Route Monitoring

## 2. RELATED WORK

The traditional approach to wireless sensor network routing include the Low-Energy Adaptive Clustering Hierarchy (Leach) Hybrid Energy-Efficient Distributed Clustering (HEED) and Energy Delay Index for Trade-off (EDIT). The algorithm proposed in this paper is based on the DUAL algorithm. This algorithm main focus is less replacement of the sensor nodes and increasing the node life time and reduced the sensor node cost.

Wireless sensor network is a collection of distributed autonomous sensors for monitoring the environmental condition, immense amount of small, low cost, self power plants that are competent of sense, compute and communicate. Recent advances in MEMS technology have enable low power and multifunctional sensor nodes that are small in size and the development of low-cost and converse in small distances [5]. Neat sensor nodes are low power procedure ready with one or more sensors a computer recollection a control bring a data lines and an actuator. A various kinds of automatic chemical biological visual thermal and attractive sensors are attached to the sensor node for measuring the property of surroundings. These sensor nodes are closely deploy within the phenomenon or shut down. The nodes are deploying randomly in set of measures to improve and keep an industry IT infrastructure in the event of failure relief operations. If any event is changed then it is sensed for communicating the organization location with the multi hop message among two end nodes is carried out through no. of intermediate nodes.

### A. Low-Energy Adaptive Clustering Hierarchy (Leach)

Low-energy adaptive clustering hierarchy (LEACH) is one of the most popular hierarchical routing algorithms for sensor networks [6,7]. The idea is to form clusters of the sensor nodes based on the received signal strength and use local cluster heads as routers to the sink. This will save energy since the transmissions will only be done by such cluster heads rather than all sensor nodes. All the data processing such as data fusion aggregation are local to the cluster. Cluster heads change randomly over time in order to balance the energy dissipation of nodes. This decision is made by the node S choosing a random number x between 0 and 1. The node becomes a cluster head for the current round if the number x is less than the following threshold:

TS=P1-P*(r mod 1P) if S ΓG0 otherwise (1)

Where P is desired percentage of cluster head nodes in the sensor network, r is current round number, and G is the set of nodes that have not been cluster heads in the last 1/p rounds.

LEACH achieves over a factor of 7 reduction in energy dissipation compared to direct communication and a factor of 4–8 compared to the minimum transmission energy routing. The nodes die randomly and dynamic clustering increases lifetime of the system. LEACH is completely distributed and requires no global knowledge of network. However, LEACH uses single-hop routing where each node can transmit directly to the cluster-head and the sink. Therefore, it is not applicable to networks deployed in large regions. Furthermore, the idea of dynamic clustering brings extra overhead, e.g. Head changes, advertisements etc., which may diminish the gain in energy consumption.

### B. Hybrid Energy-Efficient Distributed Clustering (HEED)

HEED (Hybrid Energy-Efficient Distributed Clustering) proposed in operates in a multi-hop inter-cluster wireless sensor networks. It improves LEACH protocol by selecting periodically CHs based on combination of residual energy of each node and node's neighbor degree in order to achieve power balancing and increase the network scalability and lifetime [8]. HEED takes into account the residual-energy of each node and a node that has the highest energy will be selected as CH. It also depends on the node proximity to its neighbors In the HEED protocol, the clustering process terminates in a constant number of iterations, which achieves fairly regular CHs distribution across the network and reduces control overhead between sensor nodes. HEED improves the network lifetime over LEACH. In LEACH the CH is selected randomly which may lead to rapid death of certain node. However, in HEED the CHs are selected with minimum communication cost which prolongs the nod's life time. In addition, the energy spent in clustering process is less in HEED compared to LEACH.

### C. Distance and Energy based Uneven Clustering (DEUC)

Distance and Energy based Uneven Clustering (DEUC), is a multi-hop protocol. Unlike M-LEACH it tries to alleviate the hotspot problem for the nodes that are closer to the base station. It uses the same EEUC method to select CH. However, it does not consider the linear relation between the radius of the CH, and the distance with its next hop. The authors in concluded that the larger the cluster radius, the less related data [9]. Therefore, it considers the distance from the sink node and the remaining energy of the sensor nodes to select CHs. The selected candidate CHs are grouped by their radius and for each group the candidate CHs with largest energy will be selected as CHs. Simulation results showed that DEUC performs better than EEUC.

### D. Energy Delay Index for Trade-off (EDIT)

If a multi-hop communication is used then selection of the "next hop" is also a challenging issue. If same node is selected as a "next hop" then it runs out of energy within a short period [10]. Hence, there is a need to design a CH election process which takes care of trade-off between energy and delay by selecting direct transmission or multi-hop transmission for intra-cluster and inter-cluster communication. If multi-hop transmission is used then selection of "next hop" to balance between the energy and delay is also a challenging task.

This algorithm works in rounds and each of these rounds are divided into two phases: i) Cluster Setup Phase and ii) Steady State Phase. A neighbor discovery phase executed once before the commencement of the first round [11].

## 3. ENHANCED INTERIOR GATEWAY ROUTING PROTOCOL

EIGRP stands for Enhanced Interior Gateway Protocol which allows router to share information to the neighboring routers which are within the same area[12] . Instead of sending the entire information to the neighboring router, the information which is needed are shared which reduces the workload and amount of data needs to be transmitted. EIGRP (Enhanced Interior Gateway Protocol) designed by CISCO system which can be used only in CISCO routers, but in 2013 it became open source, so it can be used in other routers. Neighbor table and Topology table are maintained by the EIGRP (Enhanced Interior Gateway Protocol)

It has five basic featured modules is as follows:

- Neighbor Discovery/Recovery
- DUAL State Machine
- Reliable Transfer Protocol
- MD5 Cryptographic Algorithm
- Protocol Dependent Module

### A. NEIGHBOR DISCOVERY/RECOVERY

The goal of any dynamic routing protocol is to learn about remote networks from other routers and to reach convergence in the routing domain. Before any EIGRP update packets can be exchanged between routers, EIGRP must first discover its neighbors. EIGRP neighbors are other routers running EIGRP on directly connected networks [13].

EIGRP uses Hello packets to establish and maintain neighbor adjacencies. For two EIGRP routers to become neighbors, several parameters between the two routers must match. For example, two EIGRP routers must use the same EIGRP metric parameters and both must be configured using the same autonomous system number.

Each EIGRP router maintains a neighbor table, which contains

a list of routers on shared links that have an EIGRP adjacency with this router. The neighbor table is used to track the status of these EIGRP neighbors.

The figure shows EIGRP routers exchanging initial EIGRP Hello packets. When an EIGRP enabled router receives a Hello packet on an interface, it adds that router to its neighbor table.

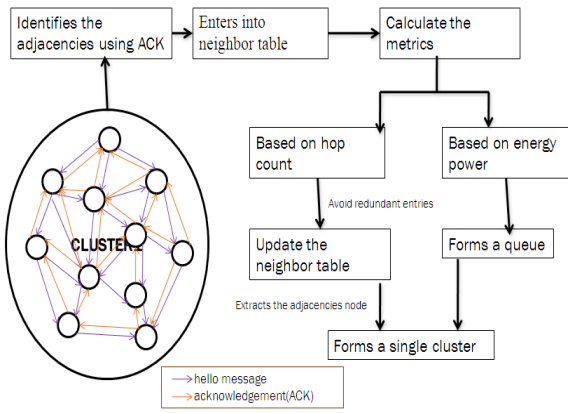


**FIGURE 3.1: Neighbor Discovery/Recovery**

**The pseudo code for neighbor discovery is as follows:**
**NEIGHBOR_DISCOVERY( )**

- SEND A HELLO MSG
- While dest_node! = first hop
- timer $t_s$ has expired
- perform network scan
- dest_nodeΓ found in scan within the cluster
- reset timer $t_s$
- RECEIVES ACK
- ENTER INTO THE NEIGHBOR TABLE
- If dest_node within cluster
- reset timer $t_s$
- equals node_energy_value(n)= link_quality_preferred(q)
- Then arranges n in descending order FIFO queue neighbor_table Γ UPDATE(n,q)

**B. DUAL FINITE STATE MACHINE**

DUAL uses three separate tables for the route calculation. These tables are created using information exchanged between the EIGRP routers. The information is different than that exchanged by link-state routing protocols [14]. In EIGRP, the information exchanged includes the routes, the "metric" or cost of each route, and the information required to form a neighbor relationship (such as number, timers, and K values). The three tables and their functions in detail are as follows.

Routing table having maximum route(s) to a destination and these routes are the successors from topology table. DUAL calculate the data expected from other routers in topology table and calculates the primary (successor) and secondary (feasible successor) routes. The primary path is typical path with least metric to attain destination, and the unnecessary path is with the second lowest cost and there may be various successors and several possible successors. Both successors and possible successors are maintained in the topology table, but only the successors are added to the routing table and used to route packets for a route to become a feasible successor, its RD must be smaller than the FD of the successor. If this possibility condition is met, there is no way that adding this route to the routing table could cause a loop.

The possible successors are additional to routing table when every successor routes to destination fail. If there is no possible successor in if all the successor routes to a destination fail, the possible successor becomes successor and topology table, a query process is initiated to look for a new route. Neighbor table is having information on further directly with connected routers and separate table exist for every sustain protocol (IP, IPX, etc.). Every entry corresponds to a neighbor with description of network interface and address. In addition, a timer is initialized to generate the periodic detection of whether connection is alive. This is complete through "Hello" packets. If a "Hello" packet is not received from a neighbor for a particular time period, the router is implicitly down and deleted from neighbor table [18].

Topology table includes metric (cost information) of every route to several destinations within the autonomous system. This information is received from neighboring routers contained in the Neighbor table. The primary (successor) and secondary (feasible successor) routes to a destination will be denoted with information in topology table with other things every entry in the topology table contains the following:

"FD (Feasible Distance)": The consideration metric of a route to a destination within the autonomous system.

"RD (Reported Distance)": The metric to a destination as present by a neighboring router. RD is used to calculate the FD, and to conclude that if the route meets the "feasibility condition".

Route Status: A route is noticeable that it is either "active" or "passive". "Passive" routes are stable and can be useful for data transmission. "Active" routes are being recalculated, and/or not available.

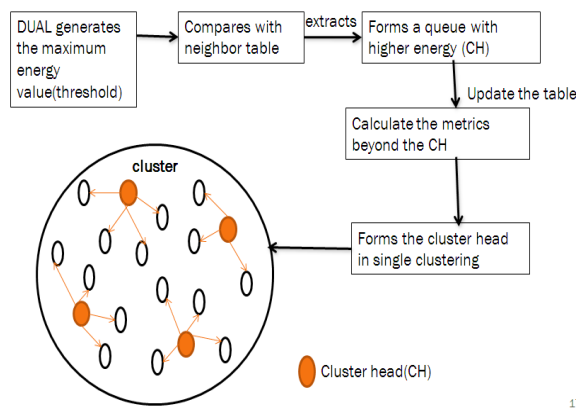


**FIGURE 3.2: DUAL OPERATION**

**The pseudo code for dual operation is as follows:**

1 if val_of_th = Energy(n) and STATE[n] = false then
2 STATE[n] := true;
3 Allocate queue(n);
4 foreach n find position on hop count;
5 receive loop-free distance n and store it in queue(n) by sending get.feasible.dist(n) // CH FORMATION
6 assign ch(n)=FIFO(queue(n))
7 each ch(n) send hello msg to first hop
8 receives update+ack
9 forms dynamic CH //UPDATE THE ROUTING TABLE
10 if STATE[ch(1)]=true then
11 STATE[ch(n<1)]=false //DYMAMIC CH ELECTION
12 if Energy(ch(1))<= val_of_th then remove from table
13 UPDATE the table.

**C. RELIABLE TRANSFER PROTOCOL**

EIGRP uses Reliable Transport Protocol (RTP) for the delivery and reception of EIGRP packets. EIGRP was designed as a network layer independent routing protocol; because of this design EIGRP cannot use the services of UDP or TCP [15]. This allows EIGRP to be used for protocols other than those from the TCP/IP protocol suite, such as IPX and AppleTalk. The figure conceptually shows how RTP operates.

Although "reliable" is part of its name, RTP includes both reliable delivery and unreliable delivery of EIGRP packets, similar to TCP and UDP, respectively. Reliable RTP requires an ac-

knowledgment to be returned by the receiver to the sender. An unreliable RTP packet does not require an acknowledgment. For example, an EIGRP update packet is sent reliably over RTP and requires an acknowledgment. An EIGRP Hello packet is also sent over RTP, but unreliably. This means that EIGRP Hello packets do not require an acknowledgment.

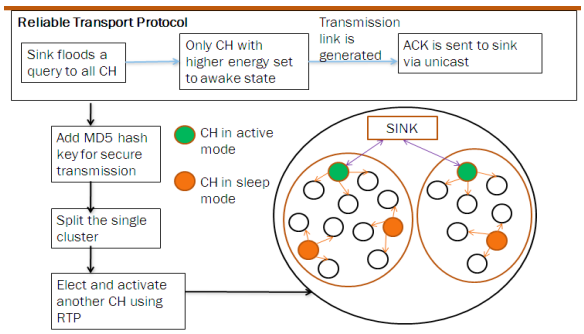


**FIGURE 3.3: RELIABLE TRANSFER PROTOCOL**

**D. MD5 CRYPTOGRAPHIC ALGORITHM**

A method to protect routing information on the network is to authenticate routing protocol packets using the Message Digest 5 (MD5) algorithm [16]. MD5 allows the routers to compare signatures that should all be the same, confirming that it is from a credible source.

**The three components of such a system include:**

Encryption algorithm, which is generally public knowledge Key used in the encryption algorithm, which is a secret shared by the routers authenticating their packets Contents of the packet itself. Pseudo code for MD5 cryptographic algorithm is as follows:

MD5 **is**
**type** Int32 **is mod 2** ** **32**;**type** MD5_Hash **is array (1** .. **4) of** Int32;

**function** MD5 **(**Input : String**) return** MD5_Hash; -- *32 hexadecimal characters + '0x' prefix* **subtype** MD5_String **is** String **(1** .. **34)**; **function** To_String **(**Item : MD5_Hash**) return**

**MD5_String;**
**end** MD5;

**E PROTOCOL DEPENDENT MODULE**

EIGRP has the capability for routing several different protocols including IPv4 and IPv6 using protocol-dependent modules (PDMs). Although now obsolete, EIGRP also used PDMs to route Novell's IPX and Apple Computer's AppleTalk network layer protocols.

PDMs are responsible for network layer protocol-specific tasks [17]. An example is the EIGRP module that is responsible for sending and receiving EIGRP packets that are encapsulated in IPv4. This module is also responsible for parsing EIGRP packets and informing DUAL of the new information that is received. EIGRP asks DUAL to make routing decisions, but the results are stored in the IPv4 routing table.

PDMs are responsible for the specific routing tasks for each network layer protocol, including:

- Maintaining the neighbor and topology tables of EIGRP routers that belong to that protocol suite
- Building and translating protocol-specific packets for DUAL
- Interfacing DUAL to the protocol-specific routing table
- Computing the metric and passing this information to DUAL
- Implementing filtering and access lists
- Performing redistribution functions to and from other routing protocols
- Redistributing routes that are learned by other routing protocols

When a router discovers a new neighbor, it records the neighbor's address and interface as an entry in the neighbor table. One neighbor table exists for each protocol-dependent module, such as IPv4. EIGRP also maintains a topology table. The topology table contains all destinations that are advertised by neighboring routers. There is also a separate topology table for each PDM.

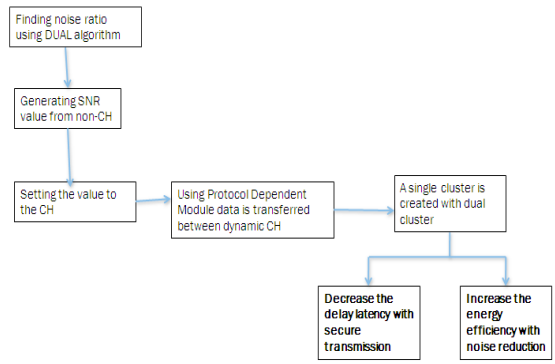


**FIGURE 3.4 PDM Operation in Clustering**

The pseudo code for the PDM operation for DUAL clustering is as follows:

//GENERATING SNR WITH DUAL

1 For n in arrange (ch);
2 SEQ(SNR) is set to 0
3 #try to calculate a SNR iter times
4 iter = 10000.
5 transmittedbits = (len(bits) – 7 * 2) * iter
6 for nodes in range (iter):
7 (signals_out,_errors, SNRs, enable) = simulate(n/1.)
8 remove noise data
//PDM FOR DUAL CLUSTERING
9 Split the routing table based on energy(ch)
10 if STATES of two CH is true else false then
11 Dynamically forwards data to sink

By using this algorithm, the sensor nodes are not only replaced, but the replacement cost is reduced, and more routing paths are reused, hence total number of sensor nodes recovered.

**4. INFERENCE AND SIMULATION**

In these networks uses 20, 40, 60, 80 and 100 nodes in simulation tests and these can be arranged in the NS2 simulator. Dimension geography of X and Y axis is 1200X1200. Here the minimum hop-count among nodes is given by using the distance between dual nodes. In a network various node pairs are selected randomly, based on each likely distance between node pair. Every node pair has different paths these may be traced by the protocol. In the network to reach the one hop neighbor we utilize all nodes. The one hop neighbor has some forwarding candidates and these can be cache by the sender using MAC interception for receiving packets. To reach the destination, the protocol uses the routing table for several possible paths. Here candidate list is maintained by the terminal. The NS2 simulation is done and we have analyzed Throughput, delay and packet delivery ratio for the flow taken. A simulation of the diffusion update algorithm as described in the experiment was designed based on 3-D space using 100 x 100 x 100 units, and the scale of the coordinate axis for each dimension was set to at 0 to 100. The transmission range of the nodes was set to 15 units. The sensors were distributed uniformly over space. There are three sensor nodes randomly distributed in 10 ×10×10 space, and the Euclidean distance is at least 2 units between any two sensor nodes. Therefore, there are 3000 sensor nodes in the 3-D wireless sensor network simulator, and the center node is the sink node.

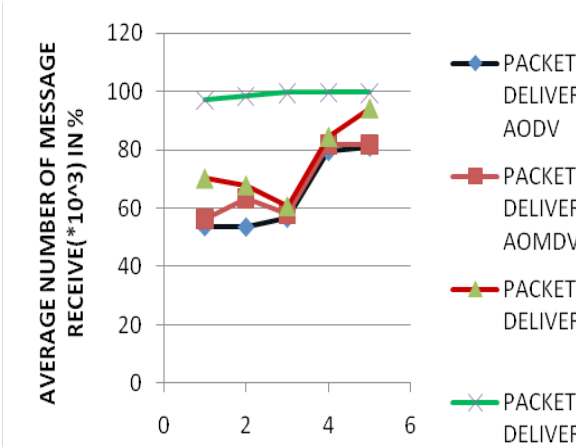


**Figure 4.1: Performance on Packet Delivery**

Figure 4.1 shows that the packet delivery of EIGRP is incredibly high compared to the existing protocols. The performance of EIGRP facilitates the protocol is constructive for applications which requires high data delivery. The considerable change in the packet delivery is when the number of nodes increase is due to the clustering methodology involved in the system.

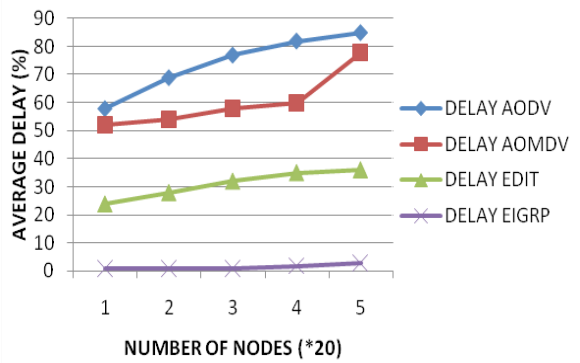


**Figure 4.2: Performance on Delay**

Average delay of the network with EIGRP protocols is given the Figure 4.2 where it outperforms other routing protocols taken for comparison. Performance of protocol is given a type in the graph but there exist a negligible delay which is considerably very small when compared with the existing routing protocols. Real time applications where delay is a significant QoS parameter to be considered can utilize the proposed protocol to attain maximum efficiency.

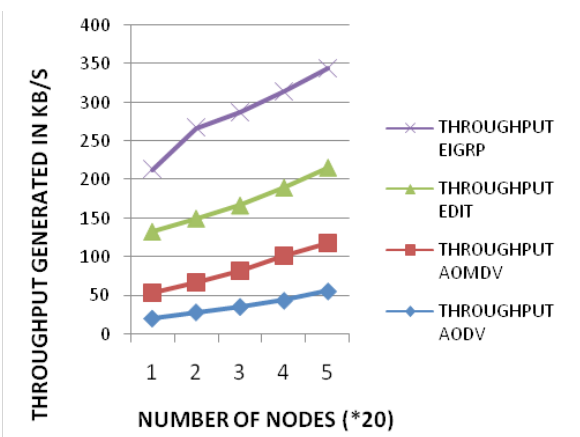


**Figure 4.3: Performance on Throughput**

When best effort service is provided where bandwidth is considered as a crucial constraint, the throughput of the system should provide complete utilization of the bandwidth. Figure 4.3 shows that EIGRP provides high throughput compared to existing protocols. One-to-one ratio between the protocols taken for comparison and EIGRP is very high.

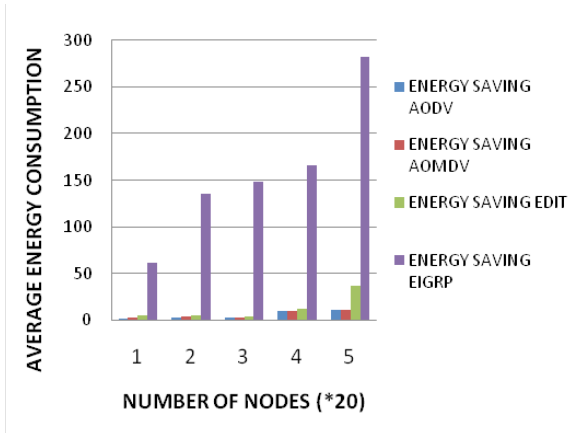


**Figure 4.4: Performance on Energy Saving**

In fig 4.4 Energy consumption is the focus of numerous QoS based protocols in progress. But it is a collective tactic to make the entire system to make use of the available energy efficiently. Battery management, task scheduling, transmission power management and diverse factors contribute to energy management. In EIGRP individual modules correlate the tasks the energy consumption is certainly less compared to the existing protocols.

## 5. CONCLUSION

The process in wireless sensor networking system is to identify a simple path for sending data to sink node from all nodes and improve its energy efficiency. In this process first it searches for sink node and selects one path from starting node to sink node. Then it reduces its latency by using RTP algorithm in which packet is delivered and also recovers the fault node. This process is repeated and MD5 hash key is added to all the packets for secured transmission. The DUAL algorithm used increases the number of CH active nodes. PDM algorithm is used for dual clustering in the network which will decrease the routing paths and replacement paths, results in increasing the life time of network. Since EIGRP includes the required QoS parameters it can be used in real time applications. The performance of EIGRP will definitely increase the efficiency of the network.

## REFERENCES

[1]. F. Akyildiz and M. C. Vuran "Wireless Sensor Networks" A John Wiley and Sons, Ltd, Publication, 2010 | [2] Yick, J.; Mukherjee, B.; Ghosal, D. Wireless Sensor Network Survey. Comput. Netw. 2008, 52, 2292–2330. | [3]. J. Pan , Y. Hou , L. Cai , Y. Shi and X. Shen "Topology control for wireless sensor networks", Proc. 9th ACM Int. Conf. Mobile Comput. Netw., pp.286 -299 2003 | [4]. E.M. Royer and C. K. Toh "A review of current routing protocols for ad-hoc mobile networks", IEEE Personal Commun., vol. 6, no. 2, pp.46 -55 1999 | [5]. H. C. Shih , S. C. Chu , J. Roddick , J. H. Ho , B. Y. Liao and J. S. Pan "A reduce identical event transmission algorithm for wireless sensor networks", Proc. 3rd Int. Conf.Intell. Human Comput. Interact., pp.147 -154 2011 | [6] Bhakti Parmar, Jayesh Munjani, Jemish Meisuria, Ajay Singh "A Survey of routing protocol LEACH for WSN"- International Journal of Scientific and Research Publications, Volume 4, Issue 1, January 2014 1 ISSN 2250-3153 | [7] Alakesh Braman , Umapathi G." A Comparative Study on Advances in LEACH Routing Protocol for Wireless Sensor Networks: A survey "-International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 2, February 2014 | [8] Bhavna Sharma, Dr. Rajiv Mhajan "Performance Evaluation of the DEEC, Teen & EDCS Protocols for Heterogeneous WSNS" International Journal of Advanced Research in Computer Science and Software Engineering Research Volume 4, Issue 10, October 2014 ISSN: 2277 128X | [9] G.Chandini, Rajavali Guntur, K. W. Rajesh Guntur. "Energy Efficient Zonal Stable Election Protocol for WSNs " - International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE) Volume 3, Issue 12, December 2014 1900 | [10] Sasikumar M , Dr. R. Anitha "Performance Evaluation of Heterogeneous HEED Protocol for Wireless Sensor Networks "International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 2, February 2014 | [11] Alia Sabri , Khalil Al-Shqeerat " Hierarchical Cluster-Based Routing Protocols for Wireless Sensor Networks – A Survey "IJCSI International Journal of Computer Science Issues, Vol. 11, Issue 1, No 2, January 2014 | [12] Ankit Thakkar, Ketan Kotecha , "Cluster Head Election for Energy and Delay Constraint Applications of Wireless Sensor Network",10.1109/JSEN.2014.2312549, IEEE Sensors Journal | [13] Thorenoor, S.G., "Dynamic Routing Protocol Implementation Decision between EIGRP, OSPF and RIP Based on Technical Background Using OPNET Modeler", April 23-25, 2010. Computer and Network Technology (ICCNT), 2010 Second International Conference. Vol. 1, pp. 191-195 | [14] B. Wu. "Simulation Based Performance Analyses on RIPv2, EIGRP, and OSPF Using OPNET." Internet: http://digitalcommons.uncfsu.edu/cgi/viewcontent.cgi?article=1011&context=macsc_wp, Aug. 20, 2011, [Mar. 15, 2013] | [15] D. Xu. "OSPF, EIGRP, and RIP performance analysis based on OPNET." Internet: www.sfu.ca/~-donx, [Mar. 15, 2013]. | [16] E.A. Mary Anita "Performance Analysis of Routing Protocols for Wireless Sensor Networks for Disaster Management"- International Journal of Computer Science and Engineering Communications- IJCSEC. Vol.2.Issue.1, February 2014. ISSN: 2347–8586 106 | [17]Khalid Abu Saud , Hatim Tahir , Moutaz Saleh ,and Mohammed Saleh ,"A Performance Comparison of MD5 Authenticated Routing Traffic with EIGRP, RIPv2, and OSPF ", The International Arab Journal of Information Technology, Vol. 7, No. 4, 2010. | [18] B.Vijay Kumar G. Hemanth Kumar Yadav, "Fault Routing Node Detection Using DUAL in | Wireless Sensor Networks" (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (1) , 2015, 558-563 |